UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**NO. 18-MJ-146**
	:	
VINCENT GALARZA,	:	
	:	
Defendant.	:	

GOVERNMENT'S MOTION FOR REVIEW AND APPEAL OF RELEASE ORDER

The United States of America, by and through its attorney, the United States Attorney for the District of Columbia, respectfully submits this Memorandum in support of its request for this Court to hear an appeal to review and overturn the Magistrate Judge's denial of the government's motion for reconsideration of release conditions and pretrial detention of the defendant, Vincent Galarza. The government submits that the defendant should be detained pending the trial of this matter pursuant to 18 U.S.C. §§ 3142(f)(1)(A) and (f)(1)(E), because there is no condition or combination of conditions that will reasonably assure the safety of any person and the community. An analysis of the factors set forth in 18 U.S.C. § 3142 leads to the conclusion that detention is appropriate.

PROCEDURAL BACKGROUND

On December 11, 2018, the defendant was arrested in the Eastern District of New York by way of a District of Columbia Complaint, charging him with one count of Conspiracy to Distribute Child Pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1). The defendant was presented in the District Court for the Eastern District of New York later that day.

The government requested that the defendant be detained pursuant to 18 U.S.C. § 3142, but the Eastern District of New York court released the defendant on conditions including home confinement with GPS monitoring, limited Internet usage, restrictions on contact with minors, and a $200,000 cash bond. The government did not appeal this decision.

On December 19, 2018, the defendant appeared before a Magistrate Judge in this Court for his initial appearance. Based on the evidence known at that time, the government consented to the defendant's request that his release conditions remain the same.

On April 22, 2019, the government filed a Motion to Reconsider Defendant's Bond Status and To Schedule a Hearing On Or Before May 3, 2019. The government filed the Motion based on newly discovered evidence (described below) pursuant to a forensic review of the electronic devices that were seized at the time of the defendant's arrest.

The Court scheduled a detention hearing for April 29, 2019. The Court heard arguments from government and defense counsel on April 29 and May 3, 2019. The government orally supplemented the record concerning the newly discovered evidence during the April 29 hearing based on recent law enforcement interviews. *See* United States v. Smith, 79 F.3d 1208, 1209-10 (D.C. Cir. 1996) (At a detention hearing, the government may present evidence by way of a proffer).

On May 3, 2019, Magistrate Judge Robinson denied the government's request to detain the defendant pending trial and ordered that the defendant remain released on conditions that included home confinement and no access to electronic devices. *See* ECF 17 at 1. The government asks this Court to review the detention determination.

FACTUAL BACKGROUND FOR CHARGED OFFENSE

A. Definition of Terms

The Tor Network

Tor is a computer network which anonymizes Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user. An "IP address" is a unique numeric address (used by computers on the internet) that is assigned to properly direct internet traffic. A publicly visible IP address can allow for the identification of the user and his/her location. To access the Tor network, a user has to install freely available Tor software, which relays only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address. There is no practical method to trace a user's actual IP address back through those Tor relay computers.

The Tor network makes it possible for a user to operate a special type of website, called "hidden services," which uses a web address that is comprised of a series of 16 algorithm-generated characters (such as "asdlk8fs9dflku7f") followed by the suffix ".onion." Websites, including hidden services, have system administrator(s) (also called the "admin(s)") who are responsible for overseeing and operating these websites.

Bitcoin

Bitcoin ("BTC") is one type of virtual currency that is circulated over the Internet. BTC is not issued by any government, bank, or company but rather is controlled through computer software. Generally, BTC is sent and received using a BTC "address," which is like a bank account number and is represented by a case-sensitive string of numbers and letters. Each BTC address is controlled through the use of a unique private key, a cryptographic equivalent of a password. Users

can operate multiple BTC addresses at any given time, with the possibility of using a unique BTC address for every transaction.

BTC fluctuates in value. Around March 5, 2018, one BTC was worth approximately $11,573.00. A typical user purchases BTC from a BTC virtual-currency exchange, which is a business that allows customers to trade virtual currencies for conventional money (*e.g.*, U.S. dollars, euros, etc.). Little to no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. However, virtual currency exchanges are required by U.S. law to collect identifying information of their customers and verify their clients' identities.

To send BTC to another address, the sender transmits a transaction announcement, cryptographically signed with the sender's private key, across the BTC network. Once the sender's transaction announcement is verified, the transaction is added to the blockchain. The blockchain is a decentralized, public ledger that logs every BTC transaction. In some instances, blockchain analysis can reveal whether multiple BTC addresses are controlled by the same individual or entity. For example, analyzing the data underlying BTC transactions allowed for the creation of large databases that grouped BTC transactions into "clusters." This analysis allowed for the identification of BTC addresses that were involved in transacting with the same addresses.

B. The Website

"The Website" was a website dedicated to the advertisement and distribution of child pornography that operated as a hidden service on the Tor network until March of 2018 when it was seized by law enforcement. On or about September 28, 2017, February 8, 2018, and February 22, 2018, from a location in Washington, D.C. law enforcement agents accessed The Website and documented its content, which is described herein. The Website was used to host and distribute video files depicting child pornography that could be downloaded by site users. The Website was

not intended to be used to upload pornography of adults, as evidenced on the upload page on The Website which clearly stated: "Do not upload adult porn."

On the video search page of The Website, there was a list of keyword search terms and the number of videos associated with the keyword. When law enforcement accessed the contents of The Website on or about February 8, 2018, it was determined that some of the top keyword search terms included "PTHC" (over 10,000 videos), "PEDO" (over 7,000 videos), "2yo%" (over 4,000 videos) and "4yo%" (over 4,000 videos).

On or about February 8, 2018, The Website indicated on its download page details that its users had downloaded video files from The Website more than a million times. On or about March 5, 2018, The Website server had over 250,000 unique video files, which totaled approximately eight terabytes of data.

Any user could create a free account on The Website by creating a username and password. Only after the user registered an account could the user browse previews of videos available for download and post text to The Website. To download videos from the site, users used "points," which were allocated to users by The Website. A registered user could earn points from The Website in several ways: (1) uploading videos depicting child pornography; (2) referring new users to The Website; (3) paying for a "VIP" account, which lasted for six months, entitled a user to unlimited downloads, and was priced at 0.03 BTC (approximately $327.60 as of March 1, 2018); or (4) paying for points incrementally (*i.e.*, .02 BTC for 230 points).[1] Points were not transferable to any other website or application.

[1] Bitcoin is volatile, and the price of bitcoin can fluctuate on an hourly basis. Between January 2017 and February 2018, for example, 1 bitcoin fluctuated in price from approximately $1,000 to $20,000 USD.

Certain persons joined the conspiracy to distribute child pornography by uploading videos to The Website. Those co-conspirators who uploaded videos of child pornography to The Website for "points" also earned additional "points" each time a customer of the site downloaded that particular video from The Website. Thus, the co-conspirators had a shared goal as part of the conspiracy—increasing the number of unique videos on The Website to drive additional traffic to it—which led to greater downloads and more points for the co-conspirators. When uploading videos, the co-conspirators would use explicit file names highlighting the content as showing the sexual exploitation of minors and would add tags that customers could search for, such as PTHC, 2yo, etc. In order to prevent duplicate videos from being uploaded, The Website operated a digital hash-value check of videos the co-conspirators uploaded in order to compare the video to other videos previously uploaded to the site. The Website did not allow a co-conspirator to upload a video whose hash value matched something previously uploaded to the site.

During the course of the investigation, law enforcement agents in Washington, D.C. accessed The Website on multiple occasions, including on or about September 28, 2017, February 8, 2018, and February 22, 2018, observed its functionality by browsing the listings on The Website, and conducted undercover purchases by downloading child pornography video files from The Website after buying points with BTC. These downloaded child pornography video files included pre-pubescent children, infants, and toddlers engaged in sexually explicit conduct. Each video available for download from The Website had a title, a description (if added by the co-conspirator), "tags" with further descriptions of the video enabling a user to more easily locate a particular category of video using The Website's search function, and a preview thumbnail image that contained approximately sixteen unique still images from the video.

C. <u>Seizure of The Website</u>

On or about March 5, 2018, South Korean law enforcement executed a search warrant at the residence of the co-conspirator administrator of The Website in South Korea. Pursuant to the search, South Korean law enforcement seized The Website's server and associated electronic storage media from the bedroom of co-conspirator administrator. South Korean law enforcement then provided to U.S. law enforcement a forensic image of the server. U.S. law enforcement subsequently obtained a search warrant to review this forensic image.

A review of the imaged data confirmed that The Website was hosted on the seized server. A review of a sample of the video files further corroborated that The Website was dedicated to the distribution of child pornography. The customer data generally identified which user was associated with which BTC payment to The Website. A review of the forensic image of the server further revealed that certain co-conspirators uploaded content to the site.

D. Identification of Co-Conspirator Galarza (A/K/A "thisthishold)

A review of the forensic image of the server revealed BTC transfers on December 17, 2016 from a BTC address to The Website's BTC address starting with 1Hrb. Subpoena returns from a virtual-currency exchange in the United States ("BTC Exchange") revealed that the source of this BTC transfers was from a BTC Exchange Account number starting with 5855 ("Subject BTC Exchange Account").[2]

[2] On December 17, 2016, the Subject Exchange Account sent approximately 0.1025 BTC and 0.005 BTC (worth about $80.97 and $3.95 respectively at the time of transactions) to a BTC mixer. A BTC mixer is a paid service that attempts to obfuscate the trail of BTC by mixing multiple clients' transactions together so that there is not a direct trail from the BTC sender to the recipient. On December 17, 2016, The Website BTC address starting in 1Hrb also received approximately 0.09882853 BTC from a mixer. It appears that the defendant was attempting to purchase a VIP account at The Website; however, he did not account for the BTC transactional fees and the mixer's fees. Thus, he had to send an additional 0.00228809 BTC (worth about $1.80 at the time of transaction) from the Subject Exchange Account to The Website. He did not use a mixer with his third transaction to The Website.

Subpoena returns from the BTC Exchange revealed that the Subject BTC Exchange Account (which sent BTC to The Website) was created on or about December 17, 2016 with the following know-your-customer data:

- registered in the name of the defendant;
- listed the defendant's date of birth and his address in Glendale, New York; and
- listed the defendant's phone number; and an email address hosted by Oath ("Subject Email Address").

As part of the BTC Exchange's legally required customer due diligence rules, the BTC Exchange confirmed the Subject Email Address and phone number by sending messages to which the user had to reply. Subpoena returns from Oath revealed that the Subject Email Address was created on December 15, 2002 and was registered in the name of defendant with same phone number that he provided when creating the Subject BTC Exchange Account.

The Subject BTC Exchange Account was funded by a Cross County Savings Bank ("CCSB") checking account ending in 0160 and a Chase Bank credit card ending in 8140. Subpoena returns revealed that both of these accounts were listed in the defendant's name. The defendant provided the same date of birth, phone number, and address when he opened these account. The defendant also provided copies of his driver's license and Social Security card when he opened his account with CCSB. Subsequent law enforcement investigation identified CCSB ATM security footage from December 26, 2017, which depicted an individual resembling the defendant's driver's license photograph accessing a CCSB ATM.

E. Defendant's (a/k/a thisthishold's) Activity on The Website

Law enforcement's review of the forensic image of the server revealed that The Website created the unique BTC address starting with 1Hrb for thisthishold, which was funded by the Subject

Exchange Account.[3] The server data revealed that between approximately May 31, 2017 and February 9, 2018, thisthishold downloaded approximately 174 videos from The Website with video file names and descriptions indicative of child pornography. Additionally, from approximately June 25, 2016 to December 21, 2016, thisthishold uploaded approximately 560 videos to The Website—all of which are videos that appear to depict child pornography.

For example, video file EA - N2016H-034.mp4 with file description "EA - N2016H-part" was uploaded to The Website by thisthishold on November 20, 2016. The video is 19 seconds long and depicts a female child, approximately five to seven years old, nude from the waist up. The child appears to be laying on her back while an adult male stands over her and masturbates his penis near her mouth until he ejaculates on her face. The video ends with a collage of photographs of the same child with semen on her face. Users of The Website downloaded this video approximately two times.

Another video, entitled 20150805201415-031.mp4 with the file description "20150805201415-part" was uploaded to The Website by thisthishold on December 20, 2016. The video is 24 seconds long and depicts a female child, approximately five to seven years old, nude from the waist down. The child appears to be laying on her back, viewing a computer tablet, while a male adult inserts the head of his penis into the child's vagina. Users of The Website downloaded this video approximately three times.

NEWLY DISCOVERED EVIDENCE WARRANTING DETENTION

A. Evidence of Defendant's Child Pornography is Now Voluminous

At the time of the defendant's arrest in New York, law enforcement executed a residential search warrant and seized several of the defendant's electronic devices, to include a self-built

[3] The Website provided each user with a unique BTC address.

computer with a Redundant Array of Independent Disks ("RAID") configuration. RAID is a sophisticated way to pair multiple drives together to improve both performance and redundancy. Due to the complex nature of the defendant's electronic configurations, it took law enforcement considerable time to forensically extract and review the approximately 1.7 million images and videos recovered from the device. However, once law enforcement was able to override the defendant's password and extract the data, a review of the self-built computer, under the username "Vincent John Galarza," identified over 500 videos and images of child pornography, the majority of which depicted sexually explicit conduct of pre-pubescent children. While the forensic review remains on-going, law enforcement has identified at least two videos that thisthishold uploaded to The Website.

B. Defendant's Production of Child Pornography

The comprehensive electronic forensic review also identified eleven videos of a 14-year old minor (CW1). CW1 has been identified as the defendant's then-girlfriend's younger sister. The defendant surreptitiously recorded the videos from two cameras between March and August 2014. Law enforcement still has over 150,000 files to review before a final number can be obtained regarding the number of videos and images the defendant illegally captured of the minor victim.

The defendant installed the first camera in CW1's bathroom. In one of the videos, his face is observed as he covertly sets up the camera. In another video, the defendant examines the angle of the camera before exiting the bathroom. This camera subsequently captured CW1 undressing and using the shower. The defendant captured at least eleven videos from this camera, which were

then edited and clipped to produce over 900 still-shot images that focus on the same minor's genitalia and pubic area.

On April 19, 2019, law enforcement interviewed W-1, a family member of CW1. W-1 confirmed the identity and age of CW1. W-1 confirmed that the location of the recordings was in CW1's bathroom in her home. W-1 further informed law enforcement that the defendant assisted W-1's family with updates to all of their electronic devices because he was computer-savvy. According to W-1, CW1 had a web-camera that had been set up on her computer in CW1's bedroom. CW1 would often complain that the web-camera would switch on and off automatically when CW1 was in the room. Law enforcement identified numerous still images on the defendant's electronic device that appear to have been captured from CW1's web camera. These depictions show CW1 in various stages of undress with her breasts exposed in her bedroom.

On April 29, 2019, law enforcement interviewed CW1.[4] CW1 identified herself as the individual depicted in the surreptitious bathroom recordings and web-camera footage. CW1 identified that these recordings and images were taken of CW1 in the privacy of her bedroom and bathroom in New York. CW1 also disclosed to law enforcement that when she was 12 years old (and the defendant was in his early to mid-20s), she began to lock her bedroom door whenever the defendant would stay at the home with W-1. CW1 explained that she began to lock her bedroom door because she would often awake in bed to find that the defendant was in bed with her. CW1 also stated that starting when she was in 5th grade (and approximately 11 years old) through her freshman year of high school, the defendant would walk by her and touch her on her buttocks.

[4] The information learned from CW1 was provided to Magistrate Judge Robinson orally at the hearing on April 29, 2019. This information was not included in the government's initial filing.

CW1 reported that she disclosed these incidents to her family members who minimized the defendant's conduct.

C. Defendant's Sextortion Of CW1

During the forensic review on the defendant's electronic devices, law enforcement identified a photograph of CW1 in her bedroom with her breasts exposed. Written on this image were words to the effect of "show me more vids or I'll show everyone."[5]

On April 29, 2019, CW1 identified herself in this image and opined that it had been taken, unbeknown to her, with her web-camera device that had been attached to her desktop computer. CW1 reported to law enforcement that at a time unknown to CW1, her desktop was remote accessed and an image of CW1 with her breasts visible appeared on her computer's screen. CW1 reported that the image on the defendant's computer appeared to be the same image that was on her hacked computer. CW1 explained that accompanying the image were typed words demanding that CW1 send more images or videos or else the photograph of her breasts would be distributed to others. Thereafter, CW1 immediately dismantled her web camera and got a new computer.

At the time, CW1 did not know who had hacked her web camera and remote accessed her desktop. The forensic review of the defendant's devices revealed that the defendant both illegally commandeered CW1's web camera by hacking her computer, and then sent her a threatening sextortion message.

D. Defendant's Assaultive Conduct

[5] The information in this section was provided to Magistrate Judge Robinson orally at the hearing on April 29, 2019. This information was not included in the government's initial filing.

CW2 is the sister of W-1 and CW1. During the recent interview of W-1, she disclosed an incident that had occurred at her home in New York on January 1, 2016. According to W-1, the defendant entered CW2's bedroom while CW2 (an adult) was asleep. CW2 woke to find the defendant standing over her bed and holding a pellet gun to her head. CW2 informed W-1 that the defendant had threatened to rape her.[6] CW2 yelled for help and W-1 came to her assistance. At that time, the defendant was removed from the house and according to W-1, he has not returned since.

During the interview with CW1, CW1 corroborated W-1's account of what happened to CW2. CW1 also added that at the time of the threatening behavior, the defendant was not wearing any clothing.

This offense was sealed in New York and thus, the government only became aware of the conduct following witness interviews.

APPLICABLE LEGAL STANDARD

The Bail Reform Act permits a judicial officer to hold an individual without bond pending trial if the officer finds clear and convincing evidence that "no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community." 18 U.S.C. § 3142(e). However, the government must prove the defendant presents a risk of flight only by a preponderance of the evidence. *United States v. Vortis*, 785 F.2d 327, 328-29 (D.C. Cir. 1986). Pursuant to 18 U.S.C. § 3142(f)(1)(A), the judicial officer shall hold a hearing on the question of detention upon the motion of the government in a case that involves a crime of violence. The offense of Conspiracy to Distribute Child Pornography, in

[6] Note, however, that in the sealed police report, CW2 provided a statement to police at the time of the offense. She stated that she could not recall what the defendant had said to her.

violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), is a crime of violence because it is a felony under Chapter 110. *See* 18 U.S.C. § 3156(a)(4)(C).

Because the instant alleged offense involves a minor victim, there is a rebuttable presumption in favor of detention. *See* 18 U.S.C. § 3142(e)(3)(E). Once a rebuttable presumption is triggered, it imposes a burden of production on the defendant "to offer some credible evidence contrary to the statutory presumption." *United States v. Alatishe*, 768 F.2d 364, 371 (D.C. Cir. 1985). "Even where defendant offers evidence to rebut the presumption, the presumption is not erased; rather, the 'presumption is incorporated into the other factors considered by this Court in determining whether to grant a conditional release and is given substantial weight.'" *United States v. Wilson*, 217 F. Supp. 3d 165, 174 (D.D.C. 2016) (quoting *United States v. Ali*, 793 F. Supp. 2d 386, 391 (D.D.C. 2011).

A motion under 18 U.S.C. § 3145(a) for review of a Magistrate Judge's "release order" requires that the Court review de novo whether conditions of release exist that "will reasonably assure the defendant's appearance in court or the safety of any other person or the community," *United States v. Hassanshahi*, 989 F. Supp. 2d 110, 113 (D.D.C. 2013). In making such determination, the Court may consider the following factors: (1) the nature and circumstances of the offense charged; (2) the weight of the evidence against the defendant; (3) the history and characteristics of the defendant; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release. *See* 18 U.S.C. § 3142(g).

This Court may reopen the question of detention "'at any time before trial' if new information is discovered that has 'a material bearing on the issue whether there are conditions of release that will reasonably assure the appearance of such person as required and the safety of any other person and the community,'" *United States v. Strong*, 489 F.3d 1055, 1060 (9th Cir. 2007)

(quoting 18 U.S.C. § 3142(f)). It is irrelevant if the government "could have discovered the [new] facts at some earlier time," nor must the new facts have "anything to do with the crime with which Defendant has been charged," *United States v. Sedano-Garcia*, No. 13-20166, 2013 WL 1395769, at *4 (E.D. Mich. Apr. 5, 2013).

ANALYSIS

The newly discovered evidence demonstrates that the defendant is a danger to the community, there are no conditions or combination of conditions that would assure the safety of the community, and he cannot rebut the presumption of dangerousness. "Put simply, Defendant's conduct is too dangerous to be managed through a supervision program." *Wilson*, 217 F. Supp. 3d at 175.

A. The Nature and Circumstances of the Offense Charged

The nature and circumstances of the charged offense favor detention. "The charged offense is extremely serious as it involves the sexual abuse of minor victims," *Wilson*, 217 F. Supp. 3d at 175. The harms to the children depicted in these videos cannot be overstated. As Congress found in enacting the Child Pornography Prevention Act of 1996, "the existence of and traffic in child pornographic images creates the potential for many types of harm in the community and presents a clear and present danger to all children." Pub. L. No. 104-208, § 121, 110 Stat. 3009. Accordingly, due to the seriousness of this charge, a violation of Section 2252(a)(2) carries a minimum term of imprisonment of five years. *See* 18 U.S.C. § 2252(b)(1).[7]

[7] Indeed, defendant's newly discovered conduct, for which he has not yet been charged, carries a minimum term of imprisonment of fifteen years. *See* 18 U.S.C. § 2252(e). This level of criminal exposure creates a significant incentive to flee. *See, e.g., United States v. Anderson*, 382 F. Supp. 2d 13, 15 (D.D.C. 2005) (citing "maximum penalty of 23 years" in support of detention); *Bikundi*, 47 F. Supp. 3d at 134 (citing substantial Guidelines estimate in support of detention).

Here, the defendant sought out and actively participated in a complex online network that fostered the mutual encouragement and promotion of the sexual exploitation of children. The defendant utilized a sophisticated method (Tor network) to evade detection of his activities. The use of such deceptive tactics contributes to a substantial risk of flight. *See, e.g., Bikundi*, 47 F. Supp. 3d at 134 (looking to defendant's "sophistication" in "set[ting] up several companies" that were used in the offense, as well as participation in "complex" fraud, in support of detention).

The defendant not only downloaded these graphic and disturbing videos, but he contributed to the growth of the conspiracy by uploading 560 videos to The Website. Accordingly, the defendant, by his very conduct, has promoted and encouraged the sexual abuse of children and warrants detention.

B. <u>The Weight of the Evidence Against the Defendant</u>

Based on the newly discovered evidence, the "support for the government's allegations appears very weighty," *United States v. Bikundi*, 47 F. Supp. 3d 131, 135 (D.D.C. 2014). The forensic review of defendant's electronic devices amplifies the weight of the evidence against him. Previously, only subpoena returns and the server data linked the Subject BTC Account in the defendant's name to the "thisthishold" user who uploaded 560 videos of child pornography to The Website in exchange for "points" to download other videos of child pornography. However, the forensic review corroborated that "thisthishold" is the defendant, as two of the videos "thisthishold'" uploaded to The Website were on the defendant's devices.

Additionally, while the defendant was originally charged without images or videos in his possession, law enforcement has now identified over 500 videos and images of child pornography on the defendant's electronic device.

Accordingly, the weight of the evidence against the defendant is sufficient and equally warrants detention. *See Wilson*, 217 F. Supp. 3d at 176 (weight of the government's evidence against defendant was "very strong," where it has by emails, the child pornography files, and statement from the defendant).

C. The History and Characteristics of the Defendant

While the defendant has no criminal history, the newly discovered evidence depicts a individual who has been actively engaged in the sexual exploitation of children and minors over the course of several years. The defendant's charged offense was not an aberration of character, but rather very much defines his character: that of a sexual predator.

Violating the trust of the family of his then-girlfriend, the defendant snuck into the minor's bathroom, secreted a recording device to capture her most intimate and personal moments, and then spent considerable time reviewing and editing these videos to screen-capture those images he was most interested in: images of her genitalia and pubic area. This alone warrants detention, because it shows an individual who knows no boundaries and who is willing to target those people in his life who trust him the most. The defendant's production and trafficking of child pornography, coupled with CW2's allegation that the defendant, while armed with a pellet gun, threatened to rape her, demonstrates an individual who presents a danger to the community.

Accordingly, the defendant's history and characteristics, to wit: a producer of child pornography and a threatened rapist, weighs in favor of detention. The defendant's "course of conduct" demonstrates that he will re-offend if he is released. *Wilson*, 217 F. Supp. 3d at 176.

D. The Nature and Seriousness of the Danger to Any Person or the Community

The defendant's sophisticated use of Tor, mixers, and RAID configurations demonstrates that the defendant is a more sophisticated offender than the average CP-collector. The defendant

has capitalized on a way to possess, distribute, and produce such material while minimizing the risk of getting caught. The use of TOR and virtual currency makes the defendant virtually impossible to monitor on pretrial release. There are no forensic tools that could be run on any electronic devices while on release to see if he has continued to access child pornography on the darknet—or whether he has commandeered another innocent minor's web-camera—nor a bank account to monitor for illicit purchases. Moreover, the instant arrest affidavit has alerted the defendant to the limited tools the government had to locate him. It took lengthy periods of blockchain analysis, the execution of a search warrant, and subsequent forensic review to detect the defendant's crime, none of which can be applied to the daily activities of the defendant while on pre-trial release.

The government understands that the defendant has been placed on the most restrictive of conditions, home confinement, with the condition that he have no electronic devices. Placing the defendant in his home fails to recognize this is "the same location [he] was in when [he] committed the crimes alleged in the Complaint," as well as the newly discovered crimes, and "therefore [it] seems unlikely that Defendant's [parents], or any third party for that matter, can effectively supervise [him]," *Wilson*, 217 F. Supp. 3d at 174–75. There is no reason to believe the defendant's parents would notify pre-trial services of any infractions. In fact, the defendant's father refused to allow law enforcement into his home at the time law enforcement was executing their arrest and search warrants, despite being shown the lawful warrants.

The defendant's production of child pornography, via sophisticated computer hacking, and sextortion threats of CW1 are the clearest indicators that he presents a significant danger to the community if he remains released. Had the government been aware of the defendant's production of child pornography, related sextortion, his threatening behavior towards CW2, and the large number of videos and images of child pornography in his possession at the time of his arrest, the

government would have appealed the Eastern District of New York's release decision and asked for his detention.

IV. **Conclusion**

A consideration of the evidence in this case and the applicable statutory factors compels the conclusion that the defendant should be detained pending trial. The defendant is not able to overcome the rebuttal presumption, particularly in light of the newly discovered evidence.

Respectfully submitted,

JESSIE K. LIU
UNITED STATES ATTORNEY

By: /s/

Lindsay Suttenberg, D.C. Bar No. 978513
Zia M. Faruqui, D.C. Bar No. 494990
Assistant United States Attorneys
555 Fourth Street, N.W.
Washington, D.C. 20001
(202) 252-7017 (Suttenberg)
(202) 252-7117 (Faruqui)
Lindsay.Suttenberg@usdoj.gov
Zia.Faruqui@usdoj.gov

CERTIFICATE OF SERVICE

I, Zia M. Faruqui, certify that, on this 5th day of May, 2019, the government filed a copy of the foregoing Motion on the Electronic Case Filing ("ECF") system and served a copy on counsel for the defendant, David Bos, Esquire, via ECF.

/s/
Zia M. Faruqui
Assistant United States Attorney